

JAP:BAS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
-----X

UNITED STATES OF AMERICA

REMOVAL TO THE
DISTRICT OF MARYLAND

-against-

Fed. R. Crim. P. 5

LEE ELBAZ,
a.k.a. "Lena Green,"

No. 17-M-821

Defendant.

-----X

EASTERN DISTRICT OF NEW YORK, SS:

JEREMY DESOR, being duly sworn, deposes and says that he is a Special Agent with the FEDERAL BUREAU OF INVESTIGATIONS ("FBI") duly appointed according to law and acting as such.

Upon information and belief, on September 14, 2017 an arrest warrant was issued by the United States District Court for the District of Maryland charging the defendant LEE ELBAZ, also known as "Lena Green," with wire fraud in violation of Title 18, United States Code, Section 1343 and conspiracy to commit wire fraud in violation of Title 18, United States Code, Section 1349. The source of your deponent's information and the grounds for his belief are as follows:

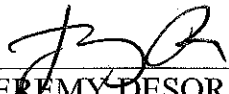
1. I have been a Special Agent of the FBI since 2004 and am currently assigned to the Washington Field Office. I am one of the agents involved in the subject underlying investigation in Maryland.

2. On September 14, 2017, a criminal complaint was filed in the United States District Court for the District of Maryland charging the defendant with wire fraud in violation of Title 18, United States Code, Section 1343 and conspiracy to commit wire fraud in violation of Title 18, United States Code, Section 1349. A copy of the complaint is attached hereto.

3. On that same date, an arrest warrant was issued by the United States District Court for the District of Maryland. A copy of the warrant is attached hereto.

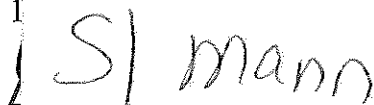
4. On September 14, 2017, at approximately 4:00 p.m., the defendant LEE ELBAZ arrived at John F. Kennedy International Airport ("JFK") in Queens, New York, aboard El Al Flight No. 7 from Tel Aviv. Prior to the defendant's arrival at JFK, the FBI alerted Customs and Border Protection ("CBP") as to the outstanding warrant for the defendant's arrest. Upon the defendant's arrival, CBP referred the defendant to secondary screening and then transferred her to the custody of FBI. The defendant was then placed under arrest. LEE ELBAZ confirmed her identity to both the FBI and CBP, and FBI determined that the defendant was the individual sought by the District of Maryland.

WHEREFORE your deponent respectfully requests that the defendant LEE ELBAZ be removed to the District of Maryland so that she may be dealt with according to law.


JEREMY DESOR
Special Agent
FBI

Sworn to before me this

1



ROANNE L. MANN
CHIEF UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

NAME: USAO 2017R00634

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

LEE ELBAZ,
a/k/a "Lena Green,"

Defendant

NO.

17-2534TJS

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A CRIMINAL COMPLAINT**

I, Michael J. McGillicuddy, being first duly sworn, state:

INTRODUCTION

1. I make this affidavit in support of an application for a criminal complaint and arrest warrant for LEE ELBAZ, also known as "Lena Green," a resident of Israel who is scheduled to travel to the United States on September 14, 2017.

AGENT BACKGROUND

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to its Washington Field Office. I have been employed by the FBI for more than 11 years. I am currently assigned to a securities fraud squad which shares the Washington Field Office's investigative responsibility for complex financial crimes. I have participated in numerous criminal investigations to include violations related to corporate fraud, securities fraud, mail fraud, wire fraud, money laundering, and obstruction of justice. Prior to joining the FBI, I was a forensic accountant for an economic consulting firm. I am a Certified Public Accountant and a Certified Fraud Examiner.

3. I am familiar with the information contained in this affidavit. This affidavit is based upon information from multiple sources—including my personal observations, witness interviews, information provided to me by regulatory agencies and other law enforcement agents and officers, documents and financial records provided by different entities and individuals, and publicly available information.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that ELBAZ has committed violations of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1349 (conspiracy to commit wire fraud) in the District of Maryland and elsewhere.

PROBABLE CAUSE

6. As explained further below, I respectfully submit that there is probable cause to believe that ELBAZ has committed violations of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1349 (conspiracy to commit wire fraud) in connection with her conduct as Chief Executive Officer (CEO) of Yukom Communications (“Yukom”), a company that operated in the binary options industry under the brand names BinaryBook and BigOption (collectively, the “Yukom Brands”). Section I provides general background on binary options, as well as information (based on the investigation to date) concerning how binary options are sold and marketed. Section II provides background on Yukom’s operations. Section III summarizes investor complaints the FBI has received to date relating to the Yukom Brands, including a complaint by an investor located in Maryland. Section IV provides specific details relating to ELBAZ’s role and conduct.

I. Background on Binary Options

7. A binary option is a type of option contract in which the payout depends on the outcome of a discrete event, typically related to whether the price of a particular asset—such as a stock or a commodity—will rise above or fall below a specified amount. Unlike standard options, investors in binary options are not being given the opportunity to actually purchase a stock or a commodity but, rather, are effectively speculating on whether its price will be above or below a certain amount at a certain time of the day. When the binary option expires, the option holder will typically receive either a pre-determined amount of cash or nothing. Binary options are sometimes referred to as “two-way” options.

8. For example, an investor may expect that the price of an individual stock will be above \$80 at 3:30 p.m. on a given day. The investor may then buy a binary option that allows her to place this bet at a cost of \$60. If, at 3:30 p.m., the stock price is \$80.01, the investor should receive an amount equal to the advertised payout. In this example, if the advertised payout was \$90, the trade would have resulted in a profit of \$30. If the price of the stock at 3:30 p.m. is \$79.99, the investor loses her \$60 investment. Investors can buy multiple binary options, which can significantly increase their returns or losses.

9. The trading of binary options is facilitated by “platform providers,” including a company named “SpotOption,” which has referred to itself on its website as “today’s leading technology platform provider.” Individuals who have worked in the binary options industry—including a former SpotOption employee—reported that SpotOption is physically based in Israel, though the “Contact Us” portion of its website shows contact information for locations in the United Kingdom, Hong Kong, and Cyprus, with no mention of Israel.

10. SpotOption and other platform providers offer a full range of services to sellers of binary options, which are referred to as “brands” or “brokers,” including the Yukom Brands (the

terms “brands” and “brokers” are used interchangeably throughout this affidavit to refer to entities engaged in the sale of binary options; the terms “broker” and “brokers” are also used to refer to certain individuals acting on behalf of these entities). Among other services, the platform providers create and determine the terms of the options that are available to trade, provide an online trading interface through which trades are placed, provide brand website templates, and provide customer relationship management software to allow brands to track relevant data for each of their investors.

11. Some binary options are listed on registered exchanges or traded on a designated contract market that are subject to oversight by U.S. regulators such as the Securities and Exchange Commission (“SEC”) and the Commodity Futures Trading Commission (“CFTC”). However, a large portion of the binary options market operates outside of these exchanges and markets. These operators typically utilize internet-based trading platforms, as was the case with the Yukom Brands. There is no evidence that the Yukom Brands facilitated trades in binary options on a legal and regulated designated contract market in the United States.

12. Binary options brands are the entities that deal directly with end customers in the United States and elsewhere to take deposits and conduct trading activity. These organizations pay a fee in exchange for utilizing the services of platform providers such as SpotOption.

13. Binary options brands rely largely on “affiliate marketers” to generate leads for potential new investors through advertisement campaigns. These campaigns often tout the ease and rapid rate at which an individual can earn large returns and feature actors posing as investors who purport to have done so. These campaigns provide the opportunity for prospective investors to submit requests for additional information.

14. After requesting additional information, prospective investors are typically contacted by a representative of a particular binary options brand. The initial contact is typically

made by a “conversion” agent from a brand—meaning a salesperson who is responsible for converting an individual into an investor by taking an initial deposit. Once an individual is converted into an investor, they are typically passed on to a brand’s “retention” department, which employs retention agents who are responsible for working with the investor going forward with the goal of obtaining additional deposits.

15. The FBI has received a large number of complaints from U.S.-based investors reporting millions of dollars in losses across many different binary options brands, including the Yukom Brands.

16. The volume of complaints and losses reported by investors to the United States government led the SEC’s Office of Investor Education and Advocacy to issue an “Investor Alert” titled “Binary Options Websites May Be Used for Fraudulent Schemes” in November 2016. The alert noted that representatives of binary options brands “may use fictitious names and tout fake credentials, qualifications, and experience.” The alert warned individuals to look out for various red flags—such as “high pressure sales tactics or threats,” “issues with withdrawals,” “constant turnover of representatives,” and “credit card abuse”—when considering whether to invest through a binary options website. The alert further stated that “in addition to perpetrating fraudulent investment schemes, the operators of binary options websites may be violating the federal securities laws through other illegal conduct.” The other conduct described in the alert included “making material misrepresentations to investors” (as well as other potential violations of federal securities laws).

17. In addition, in or around June 2017, Apple, Inc.—which manufactures and sells cellular phones popularly known as “iPhones”—updated its guidelines governing the review of proposed applications (or “apps”) developed by third parties for use on iPhones, and the company specified that “[a]pps that facilitate binary options trading are not permitted.” Public news reports

indicate that the company made this revision as a result of complaints concerning fraud in connection with the purchase and sale of binary options.

II. Operations of the Yukom Brands

18. The FBI has interviewed two individuals, Witness #1 and Witness #2,¹ both of whom formerly worked in the retention department for BinaryBook. Retention departments typically employed salespeople who contacted existing investors and solicited for larger investments. The information Witnesses #1 and #2 provided with respect to the operations of the Yukom Brands is consistent with information the FBI has learned about unregulated binary options brands in general during its investigation.

19. Witnesses #1 and #2 advised that the retention departments for BinaryBook and BigOption were operated out of the same facility in Caesarea, Israel. Witnesses #1 and #2 both stated that salespeople were instructed by management to lie to clients about their location by claiming to be located in parts of the world other than Israel.

20. Witnesses #1 and #2 both reported that Yukom employees utilized aliases when conducting business, particularly when communicating with investors. Witness #1 was instructed to choose an alias during training and to choose a name that sounded American in order to attract more investor deposits.

21. Witnesses #1 and #2 advised that SpotOption and BinaryBook worked together as needed to increase the likelihood that particular customers would lose money on trades. Other former industry insiders have also informed the FBI that SpotOption and binary options brands worked together to insure that clients who were having a high success rate of winning trades would

¹



lose future trades. The FBI has learned through interviews and a review of emails produced by Google pursuant to a search warrant issued on June 28, 2017 by the Honorable Laurel Beeler of the United States District Court for the Northern District of California, that this was done through the adjustment of customer risk settings by SpotOption. The email review has confirmed this conduct took place with respect to BinaryBook and other binary options brands. For example, on July 15, 2016, a BinaryBook representative emailed servicecenter@spotoption.com and wrote, "Please check the 2 customers below. check [sic] their risk and make modification to promise the risk is stable." The email then listed two email addresses and customer ID numbers. The reply from servicecener@spotoption.com read with respect to one customer, "[H]e is all in with risk level normal." With respect to the second customer, the email read, "[W]e well [sic] look after him and changed risk level to high."

22. According to Witnesses #1 and #2, the Yukom Brands salespeople were taught to spend as much time as needed with prospective and current investors on the phone to gain their trust, build rapport, and develop a financial profile of them. Witness #1 was instructed to do whatever was necessary to extract as much money as possible from clients. When management identified a prospective investor who had significant assets, that individual was assigned to a salesperson who had proven effective at obtaining large deposits from others in the past.

23. Unlike a company operating in a regulated market and matching a buyer and a seller, the Yukom Brands were on the opposite side of their own clients' trades, as was standard for unregulated binary options brands. This meant the Yukom Brands only made money if their customers lost money. This fact was not disclosed to clients and, in fact, representations to the contrary were made to clients in that brokers represented that they were working on behalf of clients to help the clients make money. Multiple victims interviewed by the FBI stated that they

would not have invested in the first place had they known that the binary options brands were on the opposite side of their trades.

24. According to Witnesses #1 and #2, Yukom salespeople were instructed to address client withdrawal requests at the start of each shift. The sales staff was instructed by management to take steps to delay or prevent withdrawals. Sales staff sought to convince clients to keep their money on deposit by promising positive future results or offering special investment packages that did not actually exist. According to Witnesses #1 and #2, customers who deposited funds by wire had very little chance of executing a successful withdrawal request as there was no threat of a "chargeback" as there would be with credit card deposits.

25. According to Witnesses #1 and #2, Yukom managers got involved as needed in order to prevent customer withdrawals when a salesperson was unable to do so and used whatever means necessary to prevent withdrawals. According to Witness #2, this included using false claims about clients being involved in money laundering to lock client accounts and refuse withdrawal requests.

26. According to Witnesses #1 and #2, the Yukom Brands offered bonuses to incentivize customers to deposit additional funds. These bonuses included terms that required customers to reach high levels of trade turnover before being able to make a withdrawal, which effectively locked customer accounts from withdrawals. According to Witness #1, bonuses were sometimes deposited into client accounts without the knowledge of the client in order to lock the account.

27. According to Witness #2, the Yukom Brands offered purportedly insured trades to customers. In doing so, it was represented to the customers that they would be repaid for any losses suffered in connection with the insured trades. According to Witness #2, any repayment on losses was treated as a bonus, thereby locking the client's account from withdrawals.

28. The Yukom Brands salespeople and managers received commissions based on the amount of deposits obtained. According to Witnesses #1 and #2, customer withdrawals were deducted from deposits when calculating commissions. This incentivized sales staff and managers to do everything possible to prevent withdrawals.

29. According to Witness #2, salespeople attempted to have clients sign "trade authorization forms" once an account balance exceeded \$25,000. Witness #2 likened the client signing this form to a "death sentence" because it allowed the broker to trade for the client. According to Witness #2, the broker would typically make sure the investor won some trades until the broker felt the client had reached their maximum deposit amount. At that point, the broker would execute trades in a manner designed to ensure the investor lost all of his or her money.

30. SpotOption tracked financial data for brands operating on its platform in order to calculate the amount of fees the brands had to pay to SpotOption on an ongoing basis. SpotOption produced certain records to the U.S. government, including accounting details relating to BinaryBook. According to the SpotOption records, BinaryBook received customer deposits totaling \$98.9 million from the second quarter of 2014 through the fourth quarter of 2016. According to the SpotOption records, BinaryBook returned \$19.9 million to its clients during this same time period. According to the SpotOption records, BinaryBook's "Position [Profit and Loss]" during this time period was \$80.9 million. The SpotOption records did not include accounting details for BigOption.

III. Investor Complaints

31. The FBI has received numerous investor complaints relating to BinaryBook and BigOption. The allegations in the complaints corroborate the details provided by Witnesses #1 and #2 with respect to how the Yukom Brands operated and treated their investors. The conduct

described by complainants is consistent with conduct described by complainants relating to many other unregulated binary options brands.

A. Complaints relating to BinaryBook

32. The FBI has received complaints relating to BinaryBook from approximately 33 investors alleging losses totaling more than \$1 million. These complaints included allegations of unauthorized bonuses being deposited into accounts to tie up customer funds, as well as losses suffered due to unauthorized trades made after a withdrawal request by a client. The complainants also reported an inability to withdraw funds from their accounts. Some of the complaints are summarized as follows:

Investor A

33. Investor A invested approximately \$45,000 with BinaryBook. Investor A was told by a broker that the broker made millions for his clients and won 85-95% of his trades. This broker told Investor A, "If you win, I win." The broker conducted most of the trading in Investor A's account.

34. Investor A's account grew at one point to as much as \$92,000 including bonuses. Investor A then suffered losses of approximately \$60,000 in her account. Investor A attempted to withdraw money from her account but was unable to do so. Investor A received various excuses as to why her withdrawal request was not processed. BinaryBook representatives encouraged Investor A to not withdraw her funds by telling Investor A that she would be a millionaire within a year. As of May 30, 2017, Investor A had not received any money back from BinaryBook.

Investor B

35. Investor B opened a BinaryBook account with a \$250 deposit in or around November 2015. Investor B's main broker at BinaryBook was "Mila Morales." Morales told Investor B that she was a successful trader. Over time, Investor B invested approximately

\$385,000 with BinaryBook. Morales convinced Investor B to invest additional funds with BinaryBook in part by stating that Investor B would become eligible for risk-free trades and bonuses with increased trading volume. Investor B was promised that Investor B's profits would increase if Investor B invested additional funds. Investor B felt pressured to deposit additional funds into Investor B's account.

36. Investor B engaged in what were described to him as "risk-free trades," meaning Investor B would be repaid in full if the trades lost. Investor B was informed after-the-fact that Investor B needed to increase trading volume in Investor B's account beyond a certain threshold to be eligible for repayment. Investor B felt a lot of pressure to deposit additional funds in order to be able to reach the threshold to get his money back.

37. As of February 13, 2017, Investor B was unable to access his account information on the BinaryBook website. Investor B had hired an attorney who sent multiple letters to BinaryBook, including a cease-and-desist letter and a letter requesting the return of all of Investor B's money. BinaryBook did not respond to the letters.

Investor C

38. Investor C is a resident of Gaithersburg, Maryland. All of the events described in this paragraph and the next paragraph occurred while Investor C was in Maryland. Investor C opened an account with BinaryBook in approximately August 2015 with an initial deposit of \$250. Investor C traded the money himself without success. Investor C was then contacted by a BinaryBook broker who told Investor C that BinaryBook could trade on Investor C's behalf. Investor C invested an additional \$5,000 and signed an agreement to allow a BinaryBook broker to trade on his behalf. The broker lost most or all of Investor C's money quickly.

39. Investor C was then contacted by a new broker at BinaryBook who promised a return of more than 23% on an upcoming trade. Investor C agreed to invest an additional \$5,000.

The new broker deposited \$5,100 in bonus funds into Investor C's account and promised Investor C that he would match up to another \$25,000 in deposits with bonus funds. Investor C then deposited an additional \$24,900 into his account. The broker traded Investor C's funds which resulted in losses of the entire account. Other brokers at BinaryBook then tried to convince Investor C to invest additional funds but he refused to do so. Investor C continued to communicate with BinaryBook employees until at least the end of 2015.

40. Investor C's communications with BinaryBook employees resulted in numerous electronic communications between Investor C in the District of Maryland and BinaryBook employees resulting in interstate wire transmissions. For example, on or about August 28, 2015, a BinaryBook employee emailed Investor C at his Google email account regarding bank wire transfer instructions in order to induce Investor C to make a deposit with BinaryBook. On or about November 3, 2015, a BinaryBook employee emailed Investor C at his Google email account regarding Investor C's purported "investment performance."

B. Complaints relating to BigOption

41. The FBI has received complaints relating to BigOption from approximately 18 investors alleging losses totaling approximately \$143,000. Some of the complaints are summarized as follows:

Investor D

42. Investor D invested more than 27,000AUD with BigOption. Investor D was assigned a broker who helped Investor D execute trades. The broker stopped communicating with Investor D when Investor D refused to deposit additional funds into his binary options account. Investor D then received messages from other BigOption staff members advising Investor D that he had to conduct trades on his own. Investor D attempted to withdraw his funds but was told that he could not do so because he had received a bonus and had not met the trading threshold requirement

of 30 times the bonus amount. Investor D has been unable to withdraw any of his money despite repeated attempts to do so.

Investor E

43. Investor E opened an account with BigOption by depositing \$500 on his credit card. Investor E quickly lost \$244 and stopped trading. Investor E was contacted repeatedly by BigOption brokers who attempted to convince Investor E to deposit additional funds into his account but Investor E refused to do so. Investor E attempted to withdraw the remaining balance in his account in April 2017 and received an email from BigOption stating his money could not be returned because he had not placed any trades within the last 30 days. The email stated Investor E would have to execute five trades before his money could be returned. This requirement to make a trade every 30 days had not been disclosed to Investor E previously.

IV. LEE ELBAZ

44. Witnesses #1 and #2 both advised that ELBAZ was the CEO of the Yukom Brands and reported to the owner of Yukom.

45. ELBAZ's position at Yukom has been corroborated through the review of emails produced by Google pursuant to a search warrant. The emails included multiple emails sent from lee@yukomgroup.com that were signed "Lee Elbaz" with the title "CEO" and a Yukom logo under her name.

46. ELBAZ's position was also corroborated through review of a document filed by Yukom's lawyers in connection with a court case filed in Israel by an investor naming Yukom, ELBAZ, and a Yukom salesperson as defendants. The filing was written in Hebrew and, according to a FBI translator, included a statement by Yukom's lawyers acknowledging that ELBAZ was the CEO of Yukom during the relevant time period.

47. Witnesses #1 and #2 both advised that ELBAZ utilized the alias "Lena Green." The emails produced by Google included certain emails sent to and from lena.green@binarybook.com and lena.green@bigoption.com. The FBI's review of these emails provided corroboration that ELBAZ utilized the alias Lena Green. For example:

- a. A June 30, 2016 email from lena.green@bigoption.com to BinaryBook staff was signed "Lee."
- b. An August 12, 2016 email to BinaryBook staff from lena.green@bigoption.com was signed "Lee." This email demonstrated that the individual utilizing the lena.green@bigoption.com account was in a high-level management position as the email was sent to company managers and stated, "As managers in this company I expect and demand all of you to take responsibility for your actions and the actions of your employees. I don't care how busy are you, I'm not going to accept not even one more mistake!"
- c. A series of emails exchanged between BinaryBook employees on April 6 and April 7, 2016 demonstrated that the individual utilizing the name Lena Green was the CEO of BinaryBook, a position held by ELBAZ. The email address lena.green@binarybook.com was copied on the emails, which related to how to address an issue with respect to a particular client. Prior to lena.green@binarybook.com responding to the series of emails, another BinaryBook employee wrote, "Guys, its [sic] Lena's decision since no one of us is the CEO except her, let us give her the time to answer when she see [sic] fit."
- d. ELBAZ's date of birth is a month and date known to the Affiant. On that date in 2016, several "Happy Birthday" emails were sent from BinaryBook employees to lena.green@binarybook.com.

48. I have reviewed a series of posts from ELBAZ's Facebook page with the email address `lena.green@bigoption.com` at the bottom of the posts. The posts were written in Hebrew but I have been informed by a FBI translator that the posts were aimed at recruiting new employees for the company. Photographs of ELBAZ on her Facebook page show the same individual depicted in the official photograph for the Visa authorizing ELBAZ's travel to the United States on September 14, 2017.

49. The FBI's review of emails produced by Google showed that ELBAZ was aware of the use of aliases by staff of the Yukom Brands and was in fact responsible for approving aliases for new employees. The `lena.green@binarybook.com` account received frequent emails seeking approval for "stage" names for employees. For example, on April 12, 2016, ELBAZ sent a reply from `lena.green@binarybook.com` with her approval or disapproval for stage names that were proposed for six different employees. One such employee was listed with the "Real Name" of "[Employee Name A]" and "Stage Name" of "James Harris." ELBAZ wrote next to the stage name, "[D]o not open with this name." Green approved three of the six stage names, including "Kate Williams" for an employee whose "Real Name" was listed as "[Employee Name B]."

50. Witness #1 advised that ELBAZ and other Yukom managers told Witness #1 and other brokers to lie to customers about their location.

51. According to Witnesses #1 and #2, ELBAZ oversaw frequent promotions and contests in which sales staff could earn bonuses and gifts for hitting certain deposit targets. The promotions and contests motivated the sales staff to take whatever steps were necessary to convince customers to deposit funds into their trading accounts.

52. The FBI's email review showed that ELBAZ herself was involved in the process of notifying SpotOption about "risky" customers. On August 2, 2016, a BinaryBook employee sent an email to `lena.green@binarybook.com` with the subject "Urgent." The employee wrote, "This

account – [customer HD]...in a very high risk [sic] Please talk to [SpotOption] asap!” ELBAZ replied the same day, “Done.”

53. Witness #1 advised that ELBAZ stressed the importance of preventing customer withdrawals. Witness #1 advised that ELBAZ herself, as Lena Green, communicated directly with clients as needed to convince them to keep their money invested with the Yukom Brands and/or to invest additional funds with the Yukom Brands. In doing so, ELBAZ identified herself as the CEO of the company and told Witness #1 that this made customers feel important.

54. According to Witness #1, ELBAZ bragged about her ability to soothe disgruntled customers and convince them to stay invested with the Yukom Brands. ELBAZ said the customers she dealt with would win their subsequent trades which would make them stay with the company.

55. A series of emails produced by Google corroborated the fact that ELBAZ, as Green, communicated directly with disgruntled clients. On April 27, 2016, Investor F, who appears to have been based in New Zealand, sent an email to a BinaryBook staff member stating, “...I’m about to do request for withdrawal of 20k.” After a series of emails over several days in which Investor F expressed concern over not receiving her funds, Investor F wrote on May 4, 2016, “I want to speak to the manager of compliance today Lena...I am tired of being mucked around...If I don’t hear from her I will take further action to get my money back.” The email account lena.green@binarybook.com was copied in a response to this email. ELBAZ, as Green, responded internally to the email by writing, “Its [sic]ok [sic] I agreed to take care and work with [Investor F]...you can let her talk to me even [sic] her account is under 500,000\$.”

56. On May 5, 2016, Investor F wrote to lena.green@binarybook.com with the subject “Thank you for talking to me.” The email read in part, “I hope all goes well with your day...U [sic] said binary book is regulated what’s the license number please...” ELBAZ, as Green, responded to this email without providing the license number. On May 6, 2016, ELBAZ, as Green,

wrote to Investor F, "I will trade with you... We can open 2 trade *[sic]* now against the usd."

ELBAZ, as Green, then provided additional trading advice to Investor F by email and Investor F wrote on May 6, 2016, "Thank you Lena for your help you are a very good teacher." ELBAZ, as Green, responded, "WOW *[sic]* YOU DID SO WELL...TOLD YOU... WE ARE *[sic]* THE WOMEN ARE GOOD AT TRADEING *[sic]*."

57. The tone of the emails between ELBAZ and Investor F changed by June 2, 2016, when Investor F wrote to lena.green@binarybook.com and copied others at BinaryBook. The email read in part, "So why did u *[sic]* cancel my last withdrawal when I had done over the 480k turnover for [bonus]? U *[sic]* said u *[sic]* would call me after three days off u *[sic]* didn't...Everyday *[sic]* I emailed u *[sic]* about approving my withdrawal... Why are u *[sic]* not returning my calls...I also know you aren't regulated as u *[sic]* have told me..." ELBAZ, as Green, replied to Investor F on June 7, 2016, writing, "Just to inform you, your account in under legal dept. as of now. We are not allowed to provide you with any future service. All communications will be done in front of our legal dept."

58. Emails provided to the FBI by investor Investor A also demonstrated ELBAZ's willingness to, as Green, speak with clients who had demanded withdrawals. In an email dated February 19, 2016, Investor A wrote to finance@binarybook.com, "I requested a withdrawal of \$10k now and \$5000.00 every two weeks...If you do not send me the above amount immediately I will write to British high commissioner and several other sources." On February 26, 2016, Investor A received a response from daniel.buckley@binarybook.com with lena.green@binarybook.com copied on the email. The email read, "Lena is watching this email as well , *[sic]* She would like to schedule a call with you , *[sic]* When are you available?"

59. The FBI's review of emails showed a pattern of concern within the Yukom Brands regarding fraud alerts and chargebacks with banks and an attempt to hide the fact that funds were

being deposited for investment in binary options. ELBAZ was involved in these communications. For example, on July 27, 2016, lena.green@bigoption.com was copied on an email to Yukom staff from itay@bigoption.com. The email read, "Following a couple of issues where the banks of the customers stopped the customers from sending the wire- please make sure to instruct the customers they should tell the bank (if asked) they send the funds to an investment company (and not to a binary company)." ELBAZ, as Green, replied to the email and added new recipients writing, "Adding all the rest...Make sure to explain *[sic]* your team." A BinaryBook representative replied to the email with sample wire transaction details that included a reference to "Currency trading for Binarybook." The employee wrote, "In this case can we delete – for Binarybook?" ELBAZ, as Green, responded, "Delete binary *[sic]* Put just BOOK."

60. On August 12, 2016, ELBAZ forwarded an email from lena.green@bigoption.com to Yukom managers. The original email was from itay@bigoption.com and was addressed, "Dear Lee." In the original email, Itay referenced issues with employees directing customers to send wires to old bank accounts. In forwarding the email, ELBAZ wrote, "I'm telling you that this is the last time that we have problems with wires. As managers in this company I expect and demand all of you to take responsibility for your actions and the actions of your employees. I don't care how busy are you, I'm not going to accept not even one more mistake! As of today, if we are going to have one mistake, commission will not be paid not the ET and not to the manager. Needless to say, that while the company is losing money due to these mistakes (money got stuck in the bank, account are being closed, fees for exchange rate and etc.) you got your commissions (bonuses were paid even when the company didn't get the money) – no more!!!!!!!!!!!!!"

61. On August 16, 2016, ELBAZ, as Green, forwarded an email to Yukom staff that originated from itay@bigoption.com. The original email read, "I have seen today a case where the

bank suspected the TRX² to be a fraud and declined it because the CM tries to deposit the same amount he has deposited in the past. Sometimes it's worth trying to decrease the amount a little and try again. It might work." In forwarding the email, ELBAZ wrote, "Just to remind you and make sure you are on it."

62. On August 26, 2016, ELBAZ sent an email to BinaryBook staff from lena.green@bigoption.com. In the email ELBAZ laid out the pattern of conduct within the company that was resulting in frequent chargebacks, writing:

"After checking and lot of investigation about the Big Amount Chargebacks that we get, its [sic] a pity to have the following result.

The reason we get these ChageBacks [sic] are [sic] simply because we cannot handle big amounts.

- **Conversion Convert the client**
- **Expert Trader get the client to invest Big Amounts**
- **Expert Trader are afraid of Withdrawals, hence they expose the client (or trade on their behalf)**
- **When client lose, Expert Traders give Bonuses**
- **Client now wants to withdraw but cannot as its [sic] a Bonus but client was not informed about it**
- **Client go to Finance and fight**
- **Finance decline Withdrawal**
- **Client Furious and go to the bank or lawyer**

This gets me to conclusion that we are not handling the Big Amounts Deposits and turns against us.

I am having a very bad time with the PSPs³ about it." (emphasis in original)

63. Over time, the Yukom Brands utilized many different bank accounts in various countries to receive customer deposits. The accounts were always in the name of a third party

² Based on my training and experience and the context, I believe "TRX" refers to "transaction."

³ Based on my training and experience and the context, I believe that "PSPs" refers to Payment Service Providers. Payment service providers offer companies services for accepting electronic payments via a variety of payment methods, including credit cards and bank-based payments (e.g., direct debit, bank transfers, etc.).

business rather than in the name of Yukom or the Yukom Brands. The FBI's review of the emails produced by Google showed ELBAZ sent emails to company staff with bank account details when new accounts were opened.

* * *

64. In summary, employees of the Yukom Brands, with ELBAZ as CEO, sought to obtain the maximum deposit from investors and, once that had been accomplished, took steps to ensure the investors lost the money in their accounts, thereby making money for themselves and their brand in the process. At the same time, investors were induced to deposit funds with the brokers based on misrepresentations concerning the riskiness of the investment. In sum, based on the investigation of the scheme so far, I believe the misrepresentations to investors, including at least one investor in Maryland, include at least the following: (1) false statements about the safety of the investments; (2) false statements regarding high returns that are guaranteed or very likely; (3) false statements regarding the ability to withdraw investment funds and false statements about the reasons that funds cannot be withdrawn; (4) misleading information about the location and qualifications of "brokers" assisting victims; (5) failing to disclose the brands and brokers only made money when investors lost money; and (6) failing to disclose the manipulation of the option returns by the brands and/or SpotOption.

65. Yukom salespeople and brand management, including ELBAZ, employed various tactics to prevent customer withdrawals—including promising investors that future trades would generate large returns, convincing investors to keep their funds in the account through claims about special promotional packages, depositing additional bonus funds into accounts to effectively lock the accounts, and falsely claiming they have received notice that investors were involved in money laundering and the funds could therefore not be released.


17-2534TJS

66. As detailed above, ELBAZ was directly involved in (1) approving aliases for Yukom employees; (2) communicating with SpotOption about risky clients; (3) communicating directly with clients who demanded withdrawals in order to prevent or delay the withdrawals; (4) working with Yukom staff to avoid banks and credit card payment processors detecting fraud in connection with customer deposit transactions; and (5) incentivizing sales staff to bring in the maximum amount of deposits from investors while knowing the Yukom Brands would only profit if their own clients lost money.

CONCLUSION


67. Based on the forgoing, I request that the Court authorize the attached complaint charging ELBAZ with violations of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1349 (conspiracy to commit wire fraud) in the District of Maryland and elsewhere, and issue the proposed arrest warrant.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.



Michael J. McGillicuddy
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on September 14th, 2017



Honorable Timothy J. Sullivan
UNITED STATES MAGISTRATE JUDGE

AO 442 (Rev. 01/09) Arrest Warrant

UNITED STATES DISTRICT COURT

for the
District of MarylandUnited States of America
v.LEE ELBAZ
Defendant

Case No.

17-2534TJS

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
 (name of person to be arrested) LEE ELBAZ, a/k/a "Lena Green"
 who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☒ Complaint
☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

18 U.S.C. 1343 Wire Fraud
 18 U.S.C. 1349 Conspiracy to Commit Wire Fraud

Date:

September 14, 2017

 Issuing officer's signature

City and state:

Greenbelt, MD

Hon. Timothy J. Sullivan, U.S. Magistrate Judge

Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
 at (city and state) _____

Date: _____


 Arresting officer's signature

Printed name and title

17-2534TJS

AO 442 (Rev. 01/09) Arrest Warrant (Page 2)

**This second page contains personal identifiers provided for law-enforcement use only
and therefore should not be filed in court with the executed warrant unless under seal.**

(Not for Public Disclosure)

Name of defendant/offender: _____

Known aliases: _____

Last known residence: _____

Prior addresses to which defendant/offender may still have ties: _____

Last known employment: _____

Last known telephone numbers: _____

Place of birth: _____

Date of birth: _____

Social Security number: _____

Height: _____ Weight: _____

Sex: _____ Race: _____

Hair: _____ Eyes: _____

Scars, tattoos, other distinguishing marks: _____

History of violence, weapons, drug use: _____

Known family, friends, and other associates (name, relation, address, phone number): _____

FBI number: _____

Complete description of auto: _____

Investigative agency and address: _____

Name and telephone numbers (office and cell) of pretrial services or probation officer (if applicable): _____

Date of last contact with pretrial services or probation officer (if applicable): _____